De-Quantising the Solution of Deutsch's Problem

Cristian S. Calude

Department of Computer Science
University of Auckland, New Zealand
www.cs.auckland.ac.nz/~cristian

October 27, 2006

Abstract

Probably the simplest and most frequently used way to illustrate the power of quantum computing is to solve the so-called *Deutsch's problem*. Consider a Boolean function $f : \{0,1\} \to \{0,1\}$ and suppose that we have a (classical) black box to compute it. The problem asks whether f is constant (that is, $f(0) = f(1)$) or balanced ($f(0) \neq f(1)$). Classically, to solve the problem seems to require the computation of $f(0)$ and $f(1)$, and then the comparison of results. Is it possible to solve the problem with *only one* query on f? In a famous paper published in 1985, Deutsch posed the problem and obtained a "quantum" *partial affirmative answer*. In 1998 a complete, probability-one solution was presented by Cleve, Ekert, Macchiavello, and Mosca. Here we will show that the quantum solution can be *de-quantised* to a deterministic simpler solution which is as efficient as the quantum one. The use of "superposition", a key ingredient of quantum algorithm, is—in this specific case—classically available.

1 Introduction

Consider a Boolean function $f : \{0,1\} \to \{0,1\}$ and suppose that we have a black box to compute it. Deutsch's problem asks to test whether f is constant (that is, $f(0) = f(1)$) or balanced ($f(0) \neq f(1)$) allowing *only one query* on the black box computing f.

Our aim is to show a simple deterministic classical solution to Deutsch's Problem. To be able to compare the quantum and classical solutions we will present both solutions in detail.

2 The quantum solution

The quantum technique is to "embed" the classical computing box (given by f) into a quantum box, then use the quantum device on a "superposition" state, and finally make a single measurement of the output of the quantum computation. This technique was proposed by Deutsch in the famous paper [2]; the problem was extended by Deutsch and Josza [3] and fully solved with probability one by Cleve, Ekert, Macchiavello, and Mosca [1] (see Gruska [4], or Nielsen and Chuang [6]).

Suppose that we have a quantum black box to compute f_Q which extends f from $\{0,1\}$ to the quantum (Hilbert) space generated by the base $\{|0\rangle,|0\rangle\}$. This means, that $f(0) = f_Q(|0\rangle)$ and $f(1) = f_Q(|1\rangle)$. The quantum computation of f_Q will be done using the transformation U_f which applies to two Qbits, $|x\rangle$ and $|y\rangle$, and produces $|x\rangle|y \oplus f(x)\rangle$ ($\oplus$ denotes the sum modulo 2). This transformation flips the second Qbit if f acting on the first Qbit is 1, and does nothing if f acting on the first Qbit is 0.

Here is a standard mathematically formulation of the quantum algorithm. Start with U_f and evolve it on a superposition of $|0\rangle$ and $|1\rangle$. Assume first that the second Qbit is initially prepared in the state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Then,

$$\begin{aligned} U_f\left(|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) &= |x\rangle\frac{1}{\sqrt{2}}(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= (-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned}$$

Next take the first Qbit to be $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The quantum black box will produce

$$U_f\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = \frac{1}{2}(-1)^{f(0)}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle)(|0\rangle - |1\rangle). \qquad (1)$$

Next perform a measurement that projects the first Qbit onto the basis

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

We will obtain $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ if the function f is balanced and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ in the opposite case.

To better understand the action of (1) we will present U_f in matrix form as:

$$U_f = \begin{pmatrix} 1-f(0) & f(0) & 0 & 0 \\ f(0) & 1-f(0) & 0 & 0 \\ 0 & 0 & 1-f(1) & f(1) \\ 0 & 0 & f(1) & 1-f(1) \end{pmatrix}.$$

Whatever the values of $f(0)$ and $f(1)$, the matrix U_f is unitary, so U_f is a legitimate quantum black box. Next we are going to use the Hadamard transformation H to generate a superposition of states:

$$H = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Here is the quantum algorithm solving Deutsch's problem:

1. Start with a closed physical system prepared in the quantum state $|01\rangle$.
2. Evolve the system according to H.
3. Evolve the system according to U_f.
4. Evolve the system according to H.
5. Measure the system. If the result is the second possible output, then f is constant; if the result is the fourth possible output, then f is balanced.

To prove the correctness of the quantum algorithm, we shall show that the first and third possible outputs can be obtained with probability zero, while one (and only one) of the second and the fourth outcomes will be obtained with probability one, and the result solves correctly Deutsch's problem.

To this aim we follow step-by-step the quantum evolution described by the above algorithm.

In Step 1 we start with a closed physical system prepared in the quantum state $|01\rangle$:

$$V = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

After Step 2 the system has evolved in the state (which is independent of f):

$$HV = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \times \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}.$$

After Step 3 the quantum system is in the state (which *depends* upon f):

$$U_f HV = \begin{pmatrix} 1-f(0) & f(0) & 0 & 0 \\ f(0) & 1-f(0) & 0 & 0 \\ 0 & 0 & 1-f(1) & f(1) \\ 0 & 0 & f(1) & 1-f(1) \end{pmatrix} \times \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2}-f(0) \\ -\frac{1}{2}+f(0) \\ \frac{1}{2}-f(1) \\ -\frac{1}{2}+f(1) \end{pmatrix}.$$

After Step 4, the quantum state of the system has become:

$$HU_f HV = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \times \begin{pmatrix} \frac{1}{2}-f(0) \\ -\frac{1}{2}+f(0) \\ \frac{1}{2}-f(1) \\ -\frac{1}{2}+f(1) \end{pmatrix} = \begin{pmatrix} 0 \\ 1-f(0)-f(1) \\ 0 \\ f(1)-f(0) \end{pmatrix}.$$

Finally, in Step 5 we *measure* the current state of the system, that is, the state $HU_f HV$, and we get:

1. output 1 with probability $p_1 = 0$,
2. output 2 with probability $p_2 = (1 - f_Q(|0\rangle) - f_Q(|1\rangle))^2$,
3. output 3 with probability $p_3 = 0$,
4. output 4 with probability $p_4 = (f_Q(|1\rangle) - f_Q(|0\rangle))^2$.

To conclude:

- if $f_Q(|0\rangle) = f_Q(|1\rangle)$, then $f(0)+f(1) = 0 \pmod 2$, $f(1)-f(0) = 0$; consequently, $p_2 = 1, p_4 = 0$.
- if $f_Q(|0\rangle) \neq f_Q(|1\rangle)$, then $f(0)+f(1) = 1$, $f(1)-f(0) = -1$ or $f(1)-f(0) = 1$; consequently, $p_2 = 0, p_4 = 1$.
- the outputs 1 and 3 have each probability zero.

Deutsch's problem was solved with only one use of U_f. The solution is probabilistic, and the result is obtained with probability one. Its success relies on the following three facts:

- the "embedding" of f into f_Q (see also the discussion in Mermin [5], end of section C, p. 11),
- the ability of the quantum computer to be in a superposition of states: we can check whether $f_Q(|0\rangle)$ is equal or not to $f_Q(|1\rangle)$ not by computing f_Q on $|0\rangle)$ and $|1\rangle$, but on a superposition of $|0\rangle)$ and $|1\rangle$, and
- the possibility to extract the required information with just one measurement.

3 De-quantising the quantum algorithm for Deutsch's problem

We de-quantise Deutsch's algorithm in the following way. We consider $\mathbf{Q}$ the set of rationals, and the space $\mathbf{Q}[i] = \{a+bi \mid a,b \in \mathbf{Q}\}, (i = \sqrt{-1})$. We embed the original function f in $\mathbf{Q}[i]$ and we define the classical analogue C_f of the quantum evolution U_f acting from $\mathbf{Q}[i]$ to itself as follows (compare with the formula (1)):

$$C_f(a+bi) = (-1)^{0 \oplus f(0)} a + (-1)^{1 \oplus f(1)} bi. \tag{2}$$

The four different possible bit-functions f induce the following four functions C_f from $\mathbf{Q}[i]$ to $\mathbf{Q}[i]$ ($\bar{x}$ is the conjugate of x):

$$\begin{aligned} C_{00}(x) &= \bar{x}, \text{ if } f(0)=0, f(1)=0, \\ C_{01}(x) &= x, \text{ if } f(0)=0, f(1)=1, \\ C_{10}(x) &= -x, \text{ if } f(0)=1, f(1)=0, \\ C_{11}(x) &= -\bar{x}, \text{ if } f(0)=1, f(1)=1. \end{aligned}$$

Deutsch's problem becomes the following:

A function f is chosen from the set $\{C_{00}, C_{01}, C_{10}, C_{11}\}$ and the problem is to determine, with a single query, which type of function it is, balanced or constant.

The following *deterministic* classical algorithm solves the problem:

`Given` f, `calculate` $(i - 1) \times f(1 + i)$. `If the result is real, then the function is balanced; otherwise, the function is constant.`

Indeed, the algorithm is correct because if we calculate $(i-1) \times f(1+i)$ we get:

$$\begin{aligned}
(i-1) \times C_{00}(1+i) &= (i-1)(1-i) = 2i, \\
(i-1) \times C_{01}(1+i) &= (i-1)(1+i) = -2, \\
(i-1) \times C_{10}(1+i) &= (i-1)(-1-i) = 2, \\
(i-1) \times C_{11}(1+i) &= (i-1)(i-1) = -2i.
\end{aligned}$$

If the answer is real, then the function is balanced, and if the answer is imaginary, then the function is constant.

Actually, there are infinitely many similar solutions, namely for every rational $a \neq 0$:

`Given` f, `calculate` $a(i - 1) \times f(1 + i)$. `If the result is real, then the function is balanced; otherwise, the function is constant.`

`Given` f, `calculate` $a(i + 1) \times f(1 + i)$. `If the result is real, then the function is constant; otherwise, the function is balanced.`

Of course, $\mathbf{Q}[i]$ plays no special role "by itself" in the above solution. The explanation is not deep, just the fact that classical bits are one-dimensional while complex numbers are two-dimensional. Thus one can have "superpositions" of different basis vectors.

Two-dimensionality can be obtained in various other simpler ways. For example, we can choose as space the set $\mathbf{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbf{Z}\}$, where $\overline{a+b\sqrt{2}} = a-b\sqrt{2}$. Using a similar embedding function as (2), $C_f(a+b\sqrt{2}) = (-1)^{0 \oplus f(0)}a + (-1)^{1 \oplus f(1)}b\sqrt{2}$, now acting on $\mathbf{Z}[\sqrt{2}]$, we get the solution:[1]

`Given` f, `calculate` $(\sqrt{2}-1) \times f(1+\sqrt{2})$. `If the result is rational, then the function is balanced; otherwise, the function is constant.`

[1] In fact we don't need the whole set $\mathbf{Z}[\sqrt{2}]$, but its finite subset $\{a+b\sqrt{2} \mid a,b \in \mathbf{Z}, |a|, |b| \leq 3\}$.

The correctness follows from the simple calculation of $(\sqrt{2}-1)\times f(1+\sqrt{2})$:

$$
\begin{aligned}
(\sqrt{2}-1)\times C_{00}(1+\sqrt{2}) &= (\sqrt{2}-1)(1-\sqrt{2}) = 2\sqrt{2}-3,\\
(\sqrt{2}-1)\times C_{01}(1+\sqrt{2}) &= (\sqrt{2}-1)(1+\sqrt{2}) = 1,\\
(\sqrt{2}-1)\times C_{10}(1+\sqrt{2}) &= (\sqrt{2}-1)(-1-\sqrt{2}) = -1,\\
(\sqrt{2}-1)\times C_{11}(1+\sqrt{2}) &= (\sqrt{2}-1)(\sqrt{2}-1) = 3-2\sqrt{2}.
\end{aligned}
$$

If the answer is rational, then the function is balanced, and if the answer is irrational, then the function is constant. We can classically distinguish between 1 and $3-2\sqrt{2}$ because $\sqrt{2}$ is computable.

So, again, the technique of "embedding" and "superposition" produces the desired result; this time, the computation is not only classical and simpler, but also deterministic.

4 Conclusion

We have shown a classical simple way to de-quantise the quantum solution for the Deutsch's problem. The same quantum technique, embedding plus computation on a "superposition", leads to a classical solution which is as efficient as the quantum one. More, the quantum solution is probabilistic, while the classical solution is deterministic.

How does the classical solution compare with the quantum one in terms of physical resources? A simple analogical scheme can implement the classical solution with two registers each using a real number as in the quantum case when we need just two Qbits. However, a more realistic analysis should involve the complexity of the black box, the complexity of the implementation of the embedding, as well as the complexity of the query performed.

The downside is that the superposition doesn't scale with the idea below. It is not difficult to obtain a similar solution for fixed n, but not uniformly (in each case a different function is used). Of course, uniformly the solution discussed in this note is not scalable, because n Qbits can represent 2^n states at the same time, which outgrows any linear function of n (see [3]).

Due to the fact that the number of efficient quantum algorithms is still extremely small, one can speculate that, in practice, "hybrid-like" algorithms may be preferable than pure quantum algorithms.

Acknowledgement

I am indebted to Mike Stay for illuminating discussions and criticism which contributed essentially to this note. I thank Vladimir Buzek, Jozef Gruska, Rossella Lupacchini, and Karl Svozil for various useful comments, specifically regarding “implementation” as a way to compare the quantum and classical solutions.

References

[1] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca. Quantum algorithms revisited, *Proceedings of the Royal Society of London* Series A454 (1998), 339–354.

[2] D. Deutsch. Quantum theory, the Church-Turing principle, and the universal quantum computer, *Proceedings of the Royal Society of London* Series A400 (1985), 97–117.

[3] D. Deutsch and R. Jozsa. Rapid solutions of problems by quantum computation, *Proceedings of the Royal Society of London* Series A439 (1992), 553.

[4] J. Gruska. *Quantum Computing*, McGraw-Hill, London, 1999.

[5] D. Mermin. *Quantum Computation Lecture Notes and Homework Assignments*, Chapter 2, Cornell University, Spring 2006, `http://people.ccmr.cornell.edu/~mermin/qcomp/chap2.pdf`, accessed on 7 October 2006.

[6] M. A. Nielsen, I. L. Chuang. *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2001.